ประกาศกรมโรงงานอุตสาหกรรม

เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

.....

คำนำ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจัดทำขึ้นเพื่อให้ระบบสารสนเทศของกรมโรงงานอุตสาหกรรมมีความมั่นคงปลอดภัยและมิให้ผู้ใดกระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อเผยแพร่ข้อมูลอันเป็นเท็จหรือมีลักษณะอันลามกอนาจารซึ่งอาจก่อให้เกิดความเสียหายแก่กรมโรงงานอุตสาหกรรม และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

คำนิยามศัพท์ที่ใช้ในนโยบายฉบับนี้

๑. “กระทรวง” หมายถึง กระทรวงอุตสาหกรรม

๒. “กรม” หมายถึง กรมโรงงานอุตสาหกรรม

๓. “ศูนย์สารสนเทศ” หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔. “สินทรัพย์” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศของกรมโรงงานอุตสาหกรรมภายใต้การกำกับดูแลของศูนย์สารสนเทศ

๕. “ระบบเครือข่าย” หมายถึง เครือข่ายคอมพิวเตอร์ของกรมโรงงานอุตสาหกรรมภายใต้การกำกับดูแลของศูนย์สารสนเทศ

๖. “คณะกรรมการบริหาร” หมายถึง คณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสารกรมโรงงานอุตสาหกรรม (Steering Committee)

๗. “ผู้บริหารระดับสูงด้านสารสนเทศ” หมายถึง รองอธิบดีกรมโรงงานอุตสาหกรรมที่ได้รับมอบหมายให้ทำหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer, CIO)

๘. “ผู้บริหารระดับสูงสุด” หมายถึง อธิบดีกรมโรงงานอุตสาหกรรม

๙. “ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานจ้างเหมาบริการ และเจ้าหน้าที่ประจำโครงการต่าง ๆ ของกรมโรงงานอุตสาหกรรม รวมถึงประชาชนที่เข้าใช้งานระบบสารสนเทศของกรมโรงงานอุตสาหกรรม และผู้รับจ้างที่กรมโรงงานอุตสาหกรรมมอบหมายให้ปฏิบัติงานตามสัญญา

๑๐. “สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ

๑๑. “การเข้าถึง...

๑๑. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ การเข้าถึงระบบปฏิบัติการ รวมถึงการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตสำหรับบุคคลภายนอก

๑๒. “ผู้ดูแลระบบ” หมายถึง ข้าราชการ หรือบุคคลที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศต่าง ๆ ที่ติดตั้งอยู่ภายในกรม

๑๓. “เจ้าหน้าที่กรม” หมายถึง เจ้าหน้าที่ของกรมที่มีสิทธิ์ในการเข้าออกสถานที่ อาคาร ห้อง ตามที่กำหนดในทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

๑๔. “ผู้มาติดต่อจากหน่วยงานภายนอก” หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อกับกรมในการติดตั้ง (Implement) บำรุงรักษา (Maintenance) หรือให้คำปรึกษาที่เกี่ยวข้องกับเครื่องแม่ข่าย (Server) ระบบเครือข่าย (Network) โปรแกรม (Software) ฐานข้อมูล (Database) หรืออุปกรณ์อื่นใดที่ติดตั้งอยู่ภายในห้องเครื่องคอมพิวเตอร์แม่ข่ายศูนย์สารสนเทศ

๑๕. “ผู้พัฒนาระบบ” หมายถึง ข้าราชการหรือบุคคลที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาระบบสารสนเทศและบำรุงรักษาระบบสารสนเทศให้กับหน่วยงานต่างๆ ภายในกรม

๑๖. “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๑๗. “ระบบสารสนเทศ” หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงาน สามารถนำมาใช้ประโยชน์ในตารางวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

๑๘. “เหตุการณ์ด้านความมั่นคงปลอดภัย” (information security event) หมายถึง

กรณีที่ ๑ คือ เหตุการณ์ที่เกิดขึ้นแล้วกับระบบคอมพิวเตอร์และระบบเครือข่ายของกรม

กรณีที่ ๒ คือ เหตุการณ์ที่เป็นจุดอ่อนหรือสงสัยว่าจะเป็นจุดอ่อนทั้งสองกรณี สามารถสร้างความเสียหายให้กับองค์กรได้ในลักษณะใดลักษณะหนึ่ง ซึ่งอาจส่งผลให้

- เกิดการหยุดชะงักต่อกระบวนการทางธุรกิจสำคัญ เช่น ระบบการรับแจ้ง วอ./อก.๖ เกิดการหยุดชะงัก เป็นต้น
- เป็นการละเมิดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม
- เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กรมกำหนดไว้
- เกิดภาพลักษณ์ที่ไม่ดีต่อกรม หรือทำให้สูญเสียชื่อเสียง เช่น การโพสต์ข้อความพาดพิงถึงกรมในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของกรม

๑๙. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบสารสนเทศของกรมถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

วัตถุประสงค์...

วัตถุประสงค์

๑. ประกาศกรมโรงงานอุตสาหกรรม เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ฉบับนี้จัดทำขึ้นเพื่อกำหนดนโยบายและแนวทางให้เกิดความมั่นคงปลอดภัยในระบบสารสนเทศ โดยมีขอบเขตครอบคลุมระบบสารสนเทศของกรม และมีวัตถุประสงค์เพื่อ

๑.๑ ระบบสารสนเทศเกิดความมั่นคงปลอดภัย ป้องกันการบุกรุก และความเสียหายที่มีข้อมูลในระบบสารสนเทศ

๑.๒ ผู้ใช้งานระบบสารสนเทศเกิดความมั่นใจเมื่อระบบมีปัญหา และระบบสามารถกู้คืนกลับใช้งานได้อย่างรวดเร็ว

๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้จัดทำขึ้นเป็นลายลักษณ์อักษร และได้รับการอนุมัติจากอธิบดีกรมโรงงานอุตสาหกรรมและได้เผยแพร่ให้บุคลากรทุกคนที่เกี่ยวข้องทราบและปฏิบัติ

ความรับผิดชอบของผู้บริหาร

๑. อธิบดีกรมโรงงานอุตสาหกรรม เป็นผู้ลงนามอนุมัตินโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. คณะกรรมการบริหาร มีอำนาจหน้าที่ดังนี้

๒.๑ กำหนดและทบทวนนโยบาย ตลอดจนทิศทางงานด้านสารสนเทศของกรม

๒.๒ ผลักดันให้บุคลากรทุกคนตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบสารสนเทศและปฏิบัติตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด

๒.๓ พิจารณาสนับสนุนการจัดหาทรัพย์สินต่าง ๆ เพื่อให้การบริหารจัดการและให้บริการระบบสารสนเทศมีความมั่นคงปลอดภัยและสอดคล้องกับนโยบายตามประกาศฉบับนี้

๓. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่ดูแล ควบคุม การให้บริการด้านระบบสารสนเทศให้สอดคล้องตามนโยบายและรายงานผลการปฏิบัติงานต่อคณะกรรมการบริหารตามวาระที่กำหนด

ขอบเขตของนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมโรงงานอุตสาหกรรม ดังนี้

๑. กำหนดนโยบาย แผนงาน และโครงการด้านสารสนเทศของกรม
๒. ดำเนินการเกี่ยวกับข้อมูล และสารสนเทศเกี่ยวกับโรงงานอุตสาหกรรม
๓. การปฏิบัติงาน หรือสนับสนุนการปฏิบัติงานร่วมกับหน่วยงานอื่นที่เกี่ยวข้อง
๔. จัดสร้างระบบเครือข่ายเชื่อมโยงระหว่างหน่วยงานภายในและภายนอก
๕. พัฒนาระบบการทำงานภายในให้เข้าสู่ระบบบริหารงานรัฐอิเล็กทรอนิกส์
๖. รักษามาตรฐานข้อมูลและเสถียรภาพการให้บริการสารสนเทศ
๗. ฝึกอบรมและเผยแพร่สารสนเทศอุตสาหกรรม
๘. อื่น ๆ ตามที่ได้รับมอบหมาย

การทบทวนและปรับปรุงระบบและข้อปฏิบัติต่อไปนี้ให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๑ ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) อย่างน้อยดังนี้

๑.๑ ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงาน

๑.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศที่มีเนื้อหาอย่างน้อยดังนี้

๒.๑ การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๒.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๒.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๒.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๓ การควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๓.๑ ให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๓.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๓.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๓.๕ การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มบริการอุปกรณ์และระบบเครือข่าย กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ

๓.๖ การควบคุม...

๓.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างเครือข่ายให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๓.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๔.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๔.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๔.๓ การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๔.๔ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๔.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๔.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๕ ควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

๕.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๕.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

๕.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๕.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๖ จัดทำระบบ...

ข้อ ๖ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

๖.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๖.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๖.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๖.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๖.๕ มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้

๗.๑ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) จากผู้ตรวจสอบภายในของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

๗.๒ การประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๘ กำหนดให้มีการทบทวนปรับปรุงนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ทันสมัยอย่างน้อยปีละครั้งหรือเมื่อระบบสารสนเทศมีการเปลี่ยนแปลงที่สำคัญ

ข้อ ๙ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๑๐ ให้ทุกหน่วยงานในกรมโรงงานอุตสาหกรรมถือปฏิบัติตามแนวปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศที่แนบท้ายประกาศฉบับนี้

ข้อ ๑๑ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบขับเคลื่อนการปฏิบัติตามนโยบายนี้

จึงประกาศมาเพื่อทราบและถือปฏิบัติ

ประกาศ ณ วันที่ ๒๕ ธันวาคม พ.ศ. ๒๕๖๑

(นายทองชัย ชวลิตพิเชฐ)
อธิบดีกรมโรงงานอุตสาหกรรม